

ICS

T/GXDSL

团 体 标 准

T/GXDSL 268—2025

原料运输防护技术规程

Specification for Supply Chain Risk Management

征求意见稿

2025 - - 发布

2025 - - 实施

广西电子商务企业联合会 发布

目 次

目录

前 言	II
一、引言	1
二、范围	1
三、规范性引用文件	1
四、术语和定义	1
五、基本原则	2
六、供应链风险管理体系建设框架	3
七、风险识别	3
八、风险评估	3
九、风险应对	4
十、监控、评审与改进	4
十一、信息、沟通与记录	4
十二、能力建设	4

前　　言

本文件依据GB/T 1.1-2020 《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

原料运输防护技术规程

一、引言

随着全球经济一体化的深入发展和市场竞争的日益激烈，供应链的复杂性、脆弱性和不确定性显著增加，各类风险事件频发，对企业经营、产业安全乃至国民经济稳定运行构成严峻挑战。供应链风险管理已成为企业核心竞争力的重要组成部分，也是保障产业链供应链安全稳定的关键举措。为引导和规范广西壮族自治区内各类企业，特别是中小企业，系统、科学、有效地实施供应链风险管理，提升整体抗风险能力和韧性，广西产学研科学研究院依据国家相关法律法规、政策要求和标准体系，结合广西产业特点和实际情况，组织研制本规范。本规范旨在为企业建立、实施、保持和持续改进供应链风险管理提供全面指导，促进供应链协同、稳定和高效运行，服务于广西经济高质量发展战略。

二、范围

本规范规定了供应链风险管理的术语和定义、基本原则、管理体系框架、风险识别、风险评估、风险应对、监控评审与改进、信息沟通与记录以及能力建设等方面的要求。本规范适用于广西壮族自治区内从事生产、制造、服务、贸易等各类活动的企事业单位（以下简称“组织”）建立和实施供应链风险管理。其他相关机构可参照使用。本规范关注从原材料采购到最终产品交付给顾客及后续服务的全过程，包括上游供应商、内部运营、下游客户及物流服务商等所有环节。

三、规范性引用文件

下列文件对于本规范的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本规范。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB/T 23694-2023 风险管理 术语

GB/T 24353-2022 风险管理 指南

GB/T 19000-2016 质量管理体系 基础和术语

GB/T 19001-2016 质量管理体系 要求

GB/T 35770-2022 合规管理体系 要求及使用指南

GB/T 33173-2016 资产管理 管理体系 要求

《中华人民共和国突发事件应对法》（2007年11月1日起施行）

《保障中小企业款项支付条例》（2020年9月1日起施行）

《国家发展改革委 工业和信息化部 财政部 人民银行 关于做好2023年降成本重点工作的通知》（发改运行〔2023〕567号）

四、术语和定义

GB/T 23694-2023、GB/T 19000-2016界定的以及下列术语和定义适用于本规范。

（一）供应链

组织及其上游供应商、下游客户以及相关服务提供商（如物流、仓储、金融等）构成的，以实现产品和服务提供给最终用户为目的的网络结构。

（二）供应链风险

由于供应链内部或外部的不确定性和潜在事件，对供应链的连续性、效率、成本、质量以及相关方目标产生负面影响的可能性及其后果的组合。

（三）供应链风险管理

指导和控制组织与供应链风险相关的协调活动，通常包括风险识别、风险评估、风险应对和监控等过程。

（四）风险偏好

组织在追求其价值过程中愿意承担的风险类型和水平的总体描述。

（五）风险容忍度

组织或利益相关方对目标实现过程中所能接受的偏离程度。

（六）业务连续性管理

识别对组织的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响的一整套管理过程。该过程为组织建立有效应对威胁的自我恢复能力提供了框架，以保护关键相关方的利益、声誉、品牌和创造价值的活动。

（七）供应链韧性

供应链在受到干扰事件冲击时，能够通过预防、抵御、适应和恢复，保持其基本功能并快速恢复正常运营的能力。

（八）关键供应商

其产品或服务的中断将对组织的运营、财务、声誉或履行法律责任的能力造成重大或决定性影响的供应商。

五、基本原则

组织实施供应链风险管理应遵循以下基本原则：战略性原则，供应链风险管理应纳入组织的整体战略和决策过程，与业务目标紧密结合；系统性原则，应采用系统性的方法，全面覆盖供应链各环节、各层级和相关方；动态性原则，风险管理应是持续的、适应性的过程，能够根据内外部环境变化及时调整；信息化原则，应充分利用信息技术和数据分析手段，提升风险管理的效率和精准度；协同性原则，应加

强与供应链上下游伙伴的信息共享与行动协调，共同应对风险；成本效益原则，风险应对措施的选择应考虑成本与潜在收益的平衡，追求风险管理资源的最优配置；合规性原则，应确保所有风险管理活动符合国家法律法规、行业规范及合同约定。

六、供应链风险管理体系建设框架

组织应建立、实施、保持并持续改进文件化的供应链风险管理体系。该体系应被视为组织整体管理体系的有机组成部分。最高管理者应展现领导力和承诺，确保供应链风险管理方针和目标的制定，并将其与组织的战略方向相一致。最高管理者应分配合适的资源和职责权限，确保体系的有效运行。组织应明确供应链风险管理的归口部门，如供应链管理部门、风险控制部门或综合管理部门，并规定其职责。其他相关部门，如采购、生产、物流、销售、财务、质量、信息技术等，应在其职责范围内参与并支持风险管理活动。组织应制定形成文件的供应链风险管理方针，方针应体现基本原则，为制定目标提供框架，并传达到所有相关员工。组织应针对相关职能和层次，制定可测量的供应链风险管理目标。目标应与方针保持一致，并考虑重大风险和机会，适时更新。

七、风险识别

组织应系统、持续地识别可能影响其供应链目标实现的内外部风险源、风险事件及其原因和潜在后果。风险识别应覆盖供应链全链条，包括但不限于以下类别：战略与市场风险，如宏观经济波动（例如，考虑广西地区面对东盟市场的汇率波动风险）、产业政策变化、市场需求突变、竞争格局演变、技术革新替代等；运营风险，如供应商失败（特别是对广西特色农产品加工、汽车制造、高端金属材料等关键产业单一来源供应商的依赖）、生产中断、产能不足、库存失衡、物流延误或中断（例如，应对广西雨季可能引发的道路交通中断）、质量控制失效、信息技术系统故障等；财务风险，如采购价格剧烈波动、汇率利率风险、客户信用风险、付款违约（参照《保障中小企业款项支付条例》相关要求）、融资困难等；合规与法律风险，如贸易壁垒（如涉及跨境供应链）、环保法规加严、知识产权纠纷、合同争议、数据安全与隐私保护违规等；环境与社会风险，如自然灾害（广西需重点关注洪涝、台风、地质灾害等）、疫情等公共卫生事件、政治动荡、社会责任缺失（如劳工权益问题）等。识别方法可包括但不限于：流程分析、情景分析、头脑风暴、德尔菲法、检查表法、SWOT分析、供应链映射、历史数据分析、专家访谈、行业基准比较等。组织应建立并维护一个全面的供应链风险登记册，记录已识别的风险及其特征。

八、风险评估

对已识别的风险，组织应进行分析和评价，以确定风险的优先级，为决策提供依据。风险分析包括评估风险发生的可能性（概率）和后果（影响）的严重程度。可能性与后果的等级划分可由组织根据自身情况确定，通常采用三级（如高、中、低）或五级量表。后果的衡量维度应包括对运营、财务、安全、环境、声誉及法律责任等方面的影响。组织应结合自身风险偏好和容忍度，对风险进行评价，通常通过将可能性和后果相结合，形成风险等级（如重大风险、较大风险、一般风险、低风险）。风险矩阵是常用的评价工具。在风险评估过程中，应特别注意对关键供应商的风险评估。关键供应商的识别标准可包括采购金额占比、物料或服务的稀缺性、替代难度、交货周期等因素。对关键供应商，应进行更深入的评估，内容可涵盖其财务状况、运营稳定性、质量控制体系、业务连续性计划、地理位置风险、社会责任表现等。风险评估应是动态过程，当内外部环境发生重大变化或根据设定的评审周期（建议至少每年进行一次全面评估）时，应重新进行评估。

九、风险应对

基于风险评估的结果，组织应选择并实施一种或多种风险应对措施。风险应对策略主要包括：规避风险，即通过放弃或改变可能引致风险的活动来消除风险源，例如，停止与高风险地区的业务往来，更换不合格供应商；降低风险，即采取措施降低风险发生的可能性或减轻其后果，这是最常用的策略，例如，实施供应商多元化战略（对重大物料，建议至少在广西区内外各发展一家备份供应商），建立安全库存（可根据历史数据设定，如对于某类关键零部件，保持不低于 15 天平均需求量的安全库存），投资于备用产能或替代技术，加强合同管理中的风险条款（如违约金、不可抗力条款），推行供应链金融以稳定供应商资金流；分担风险，即通过合作或协议将部分风险转移给其他方，例如，购买财产保险、运输保险，与供应商签订价格联动协议，采用外包非核心业务；承受风险，即在对风险进行评价后，决定不采取任何措施改变其可能性或后果，通常适用于风险等级在组织容忍度之内的情况。无论选择何种策略，都应制定具体的风险应对计划，明确责任主体、所需资源、时间安排和预期效果。对于重大风险，应准备应急预案或业务连续性计划。应急预案应明确突发风险事件发生时的应急指挥体系、响应流程、处置措施、资源保障和沟通机制。业务连续性计划应识别关键业务过程及其恢复时间目标（RTO）和恢复点目标（RPO），并制定相应的恢复策略和步骤。

十、监控、评审与改进

组织应建立监控机制，对供应链风险状况、风险应对措施的实施效果以及内外部环境的变化进行持续跟踪。监控活动可包括：关键风险指标（KRIs）的监测，如供应商准时交货率（目标可设定为不低于 98%）、库存周转天数、供应链总成本波动、订单履行周期等；定期供应商绩效评审；市场信息和情报收集；审计与检查。组织应定期（如每季度或每半年）对供应链风险管理体系建设进行评审，以确保其持续的适宜性、充分性和有效性。评审输入应包括：风险登记册更新情况、风险应对计划执行状态、监控结果、已发生的风险事件及其处理教训、相关方反馈、法律法规变化等。评审输出应包括：体系改进决策、风险管理方针和目标的变更、资源需求调整等。组织应基于监控和评审的结果，以及风险事件的经验教训，采取适当的纠正和预防措施，以持续改进供应链风险管理的有效性。改进活动应致力于提升供应链的韧性、效率和成本效益。

十一、信息、沟通与记录

有效的信息和沟通是供应链风险管理成功的关键。组织应建立、实施并保持一个内外部信息沟通的过程。内部沟通应确保各级员工理解其在供应链风险管理中的角色和责任，并能够及时上报风险信息。外部沟通应与供应商、客户、物流伙伴、监管机构等相关方进行，内容可包括风险期望、合同条款、绩效要求、预警信息以及突发事件通报等。沟通应确保信息的准确性、及时性和透明性。在保护商业机密的前提下，鼓励与关键伙伴共享适当的风险信息，以协同应对。组织应重视信息技术在风险管理中的应用，如采用供应链可视化平台、供应商关系管理（SRM）系统、企业资源计划（ERP）系统的高级分析功能等，以增强风险洞察力和响应速度。组织应保留必要的成文信息，作为供应链风险管理有效运行的证据。记录可包括：风险管理方针、目标、程序、风险登记册、风险评估报告、风险应对计划、应急预案、会议纪要、培训记录、评审报告等。记录的保存和管理应符合组织的信息管理制度和相关法规要求。

十二、能力建设

组织应确保所有承担供应链风险管理职责的人员具备相应的能力。能力基于适当的教育、培训或经验。组织应：确定这些岗位所需的能力；提供培训或采取其他措施（如导师制、岗位轮换）以满足能力需求；评价所采取措施的有效性；确保员工认识到其活动的相关性和重要性，以及如何为实现目标作出贡献。培训内容应涵盖供应链风险管理的基本概念、本规范的要求、风险识别与评估方法、应急预案演练等。组织应考虑将供应链风险管理知识纳入新员工入职培训和各级管理人员的常规培训计划。广西产学研科学研究院可依托自身优势，为企业提供专业的培训、咨询和最佳实践分享服务，助力区域整体风险管理水平的提升。
